REMARKS

Applicant has carefully reviewed and considered the Office Action mailed on October 1, 2003, and the references cited therewith.

Claims 1, 7 and 14 are amended, and new claim 17 is added; as a result, claims 1-17 are now pending in this application. Please not that claim 14 was amended to add a missing word, and not to distinguish over any of the cited art.

§103 Rejection of the Claims

Claims 1-9 were rejected under 35 USC § 103(a) as being unpatentable over Benson (EP 936530). Claim 1 has been amended to add the limitation that the virtual smart card agent includes a user authentication interface for use by a user in entering a one-time password and that the virtual smart card agent authenticates the user using the one-time password.

Benson describes a virtual smart card system. Benson's virtual smart card system derives two symmetric keys from the owner's password. The first key is an authentication key and the second key is a protection key. The authentication key is used to securely identify the owner to the virtual smart card server. The protection key is used to encrypt protected information that the virtual smart card uploads to the virtual smart card server and to decrypt protected information that the virtual smart card downloads from the virtual smart card server. Benson, col. 6, paras. 21 and 22.

Applicant teaches that one advantage of smart cards is that they provide two-factor authentication. That is, the user proves his identity by presenting something he has (i.e., the card with its private key) and something he knows (i.e., the card's PIN). Applicant contrasts this to simple passwords, which provide only single-factor authentication and are, therefore, "vulnerable to any number of well known password guessing attacks." Specification, p. 5, lines 3-12.

Applicant teaches that one way to approximate the stronger protection of two-factor authentication provided by a smart card implementation is to use one-time passwords generated by an authentication token. The user proves his identity by presenting something he has (i.e., the one-time password generated by the authentication token) and something he knows (i.e., the token's PIN). Specification, p. 5, lines 22-28.

A one-time password, even one generated without the authentication token, provides additional security over the simple password described by Benson. For one, it is difficult to discover a one-time password. In addition, the authentication function described by Applicant operates independently of the smart card emulation, allowing the system designer to strengthen the authentication piece of the system without impacting the smart card emulation. This contrasts to Benson, who generates and uses an authentication key from a simple password as part of smart card emulation.

The Examiner stated that "the authentication module (agent) must in fact communicate with the VSC server in order to maintain a record of who is currently using their VSC. Hereafter the agent will be considered part of the VSC." Applicant respectfully disagrees with this interpretation of the claim language. In fact, as noted above, having an authentication process that is separate from the virtual smart card process is an advantage. The system designer can strengthen the authentication piece of the system without impacting the smart card emulation. As noted above, this contrasts to Benson, who generates and uses an authentication key from a simple password as part of smart card emulation.

Claims 1-9, as amended, do distinguish over Benson. New claim 17 is dependent of claim 1 and distinguishes over Benson for the reasons described above. Reconsideration of claims 1-9, and consideration of new claim 17, is respectfully requested.

Claims 10-16 were rejected under 35 USC § 103(a) as being unpatentable over Benson (EP 936530) in view of Handbook of Applied Cryptography.

The Examiner stated that "Benson teaches a method of authenticating users using a one time random password". Applicant respectfully submits that the section the Examiner cites describes authentication of the Virtual Smart Card process, not authentication of the user as described by Applicant and claimed in claims 10-13. Reconsideration of claims 10-13 is respectfully requested.

With regard to claims 14-16, Applicant teaches at p. 9, lines 7-29, and claims in claim 14-16, a system capable of handling multiple forms of authentication, including authentication with actual smart cards. As described by Applicant, the principal components of this architecture are the public key authentication client, the authentication server and an LDAP compliant directory service. During login, the public key authentication client connects to authentication server.

The public key authentication client receives a challenge issued by the authentication server, signs the challenge with a digital signature representing a user and sends the digital signature of the challenge back to the authentication server. The authentication server receives the digital signature of the challenge and verifies the digital signature with a public key retrieved from the directory service.

Benson is described above. As noted above, Benson bases user authentication on a hash of a simple password, generating an authentication key from a hash of the user's password. The VSC server of Benson is, as the Examiner noted, the authentication server. Benson does not, however, describe the use of a directory service (such as an LDAP directory service) to store public keys, nor a challenge/response authentication mechanism based on the public keys stored in the directory service, both of which are described by Applicant and claimed in claims 14-16.

HSC teaches that public-key techniques can be used for challenge-response based identification. As the Examiner notes, HSC teaches that a user can demonstrate knowledge of his or her private key by digitally signing a challenge with his or her private key. Neither Benson nor HSC, however, describe the use of a directory service (such as an LDAP directory service) to store public keys, nor a challenge/response authentication mechanism based on the public keys stored in the directory service, both of which are described by Applicant and claimed in claims 14-16. Reconsideration of claims 14-16 is respectfully requested.

CONCLUSION

Applicant respectfully submits that the claims are in condition for allowance. Reconsideration of claims 1-17 and notification of allowance is earnestly requested. The Examiner is invited to telephone Applicant's attorney at (612) 373-6909 to facilitate prosecution of this application.

If necessary, please charge any additional fees or credit overpayment to Deposit Account No. 19-0743

Respectfully submitted,

LAWRENCE SMITH ET AL.

By their Representatives,

SCHWEGMAN, LUNDBERG, WOESSNER & KLUTH, P.A.
P.O. Box 2938
Minneapolis, MN 55402
(612) 373-6909

Date March 1, 2004

By Thomas F. Brennan
Thomas F. Brennan
Reg. No. 35,075

CERTIFICATE UNDER 37 CFR 1.8: The undersigned hereby certifies that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail, in an envelope addressed to: Commissioner of Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on this 1st day of March, 2004.

THOMAS F. BRENNAN
Name

Thomas F. Brennan
Signature